REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
18-05-2004	FINAL	

4. TITLE AND SUBTITLE

The Fleeting Nature of Information Superiority

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

CDR Rodney E. Malloy

Paper Advisor (if Any): LtCol Derrill T. Goldizen

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The United States of America has seen vast growth in the information element of power. This paper will contrast the profound impacts of information-based warfare and information warfare on modern U.S. war fighting. The idea of information superiority becoming a key enabler for U.S. operational success will be examined. War fighting concepts will be discussed in the context of information superiority, leading to the identification of critical vulnerabilities. Finally, a strategy will be outlined to quantify these vulnerabilities and lead to development of operational war fighting concepts to achieve information superiority verses an information age adversary.

15. SUBJECT TERMS

INFORMATION OPERATIONS, INFORMATION WARFARE, INFORMATION-BASED WARFARE, CENTER OF GRAVITY, CRITICAL VULNERABILITY, COMMAND AND CONTROL WARFARE, ASYMMETRIC WARFARE

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		17	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, RI

The Fleeting Nature of Information Superiority

By

Rodney E. Malloy
CDR USN

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

18 May 2004

Introduction: The Fleeting Nature of Information Superiority

The U.S. military has pioneered the application of several new information technologies in order to significantly increase the tempo of operations to overwhelm an adversary. These advances were evident in the ability of outnumbered U.S. forces to achieve military objectives in Kosovo, Afghanistan and Iraq. During these conflicts, U.S. information dominance has been virtually uncontested at the operational level of war. Two factors are at play to explain this phenomenon: the emergence of the information age and the end of the Cold War. These conditions have driven significant technological change in the way that U.S. forces are employed, during an era in which the U.S. military has no conventional peer. It is inevitable that emerging powers will attempt to deny information superiority to U.S. forces in order to achieve an asymmetric advantage during crisis or war against the U.S. military.[1]

Information superiority is defined as, "that degree of dominance in the information domain which permits the conduct of operations without effective opposition."[2] Due to the lack of a perceived threat and no large-scale information battles to learn from, gaining and maintaining information superiority is often overlooked as an operational objective. Air, maritime, and land superiority are often principle objectives of operational war fighting, but information superiority is often not explicitly addressed. As a relatively new concept, information superiority has not received the proper scrutiny to define inter-relationships with

[1] Joint Chiefs of Staff, An Evolving Joint Perspective, US Joint Warfare and Crisis Resolution in the 21st Century, Joint Requirements Oversight Council Memorandum 022-3 (Washington, D.C.: 28 January 2003), 2-4.

[2] Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02 (Washington, D.C.: 12 April 2001 (as amended through 5 June 2003)), 255.

traditional warfare methods to enable rapid decisive operations. Further, the use of information itself from a supported perspective is not well understood.[3]

Information capabilities are generally decentralized across networks, so the most likely method of attack will be within the information domain, or cyberspace, using information operations as a central strategy.[4] Information-enabled forces will battle for information superiority by disrupting critical enemy processes on unclassified and classified networks, by physically destroying information systems, by altering public perceptions via the media, and by influencing political decisions in public and private forums.[5]

The thesis of this paper is that information superiority cannot be assumed against an information age adversary. The U.S. lead in this evolving area of warfare will be challenged in the near term. Any assumption by an operational planner that information superiority will be achieved uncontested is flawed. The concept of information superiority will be dissected to determine what U.S. capabilities might be attacked from an adversary perspective. Examination of the vulnerabilities of U.S. information-based capabilities will lead to identification of critical vulnerabilities. A recommendation for the establishment of a professional information warfare red team will be outlined.

The Emergence of the Information Age

In 1980, Alvin Toffler first published his account of the emergence of a new form of economy and society based on the power of information. He argued that information technologies would revolutionize social structures, wealth generation, and, subsequently,

[3] The author is a U.S. Navy Commander with joint, numbered fleet, carrier strike group and shipboard experience related to information operations.
[4] Information Operations are actions taken to affect adversary information and information systems while protecting one's own information and information systems. Department of Defense Dictionary, 254.
[5] David Alperts, Information Age Transformation: Getting to a 21st Century Military DOD Command and Control Research Program (Washington, DC: June 2002), 43-45.

power. This model would transform some societies from agrarian (First Wave) or industrial (Second Wave) to information (Third Wave) societies.[6] Evidence of Toffler's assertions suggests that his insights were correct. The world economy has transformed over the last 25 years due to the rising influence of information-based markets to create a global economy. The power of the media has been transformed due to the ability to share information instantaneously. Social institutions have been transformed, as widely dispersed peoples can communicate towards common objectives over the internet. These examples are all indicators of the rise of information as a central element to the social, economic, and political landscape. As the world's mightiest industrial power, the United States has been the biggest benefactor of this phenomenon, transforming business practices and creating new sectors of the economy. No other state or institution has kept pace with the United States in this realm.

In 1993, Mr. and Mrs. Toffler published a companion to his earlier work, War and Anti-War, which continued the theme that the information age had arrived and transformed economic societies. The basic premise of this second study was that societies wage war in the same manner that they accumulate wealth. Against agrarian societies, war is waged by burning crops, thereby denying the enemy the ability to feed his troops and citizens. Wars waged against industrial societies are characterized by destroying large armies equipped by industrial age assembly lines. Mass-on-mass and maneuver warfare dominate the state of the art. Toffler argued that the information age would herald a new form of warfare that could pit the information power bases of information age societies against each other. These wars

[6] Alvin Toffler, The Third Wave (New York: William Morrow and Company, 1980), 366-374

would be characterized by new war-forms that attacked information infrastructures, using control of information as the decisive objective.[7]

Arguably, there are already indications that many of Toffler's assertions were correct. Al Qaeda's ability to execute a worldwide campaign to promote political ideas using a small, networked force is evidence of the kind of threat emerging in the information age.[8] Another example is the ability of Somali warlord General Aideed to oust the U.S. military ostensibly through the use of simple tactics reliant upon cell phones to mass force against U.S. troops cornered on the ground, and most importantly using the media to erode public will and create questions of mission legitimacy.[9]

Military Use of Information as an Enabler and as a Weapon

The U.S. military is by far the largest and most sophisticated in the world. Even though significant information capabilities have been integrated into the force, it remains a high tech industrial age military that relies upon stove-piped organizations to accomplish military objectives. True information age force structures would attempt to capitalize on the inherent decentralized nature of a network to maximize the effectiveness of the force. The institutions that made the U.S. military the most potent in the world may not be best organized to deal with threats in the information age.[10]

---

[7] Alvin Toffler and Heidi Toffler, War and Anti War: Making Sense of Today's Global Chaos (New York: Warner Books, 1993), 35-92.

[8] Bruce Berkowitz, The New Face of War: How War Will Be Fought in the 21st Century (New York: The Free Press, Simon & Shuster, 2003), 9-22.

[9] Rick Brennen and R. Evan Ellis, Information Warfare in Multilateral Peace Operations: A Case Study of Somalia (Washington D.C.: Science Applications International Corporation, 18 April 1996), ii-iii.

[10] David S. Alberts and Richard E. Hayes, Power to the Edge: Command and Control in the Information Age, DOD Command and Control Research Program (Washington DC: June 2003), 53-64.

The integration of information technology into military operations has enabled smaller forces to achieve objectives by optimizing time and space factors to achieve decisive advantage in battle. These advantages span the full range of military disciplines to include: intelligence, surveillance, reconnaissance, precision strike, ground maneuver, maritime operations, and air warfare. The cumulative effect of this information advantage is an unprecedented speed of command and a shared awareness for U.S. forces across several echelons and services. All of the above describes information-based warfare, which is an optimization of industrial age warfare using information as an advantage.[11]

Information operations are the next evolutionary step in using information offensively and defensively in order to achieve a particular objective. The related disciplines of psychological operations, military deception, operational security, electronic warfare and computer network operations constitute the pillars of information operations during crisis, referred to as information warfare. These disciplines are supported by intelligence, physical destruction, public affairs, and civil affairs.[12] Offensive and defensive information operations are distinct from information-based warfare in that the objective is achieved by manipulating the information itself rather than using information to enable fires or maneuver.

Although these concepts are relatively mature, practice has proven that application is much more complex than it appears on the surface. One attribute of an information-enabled society is the relative sophistication of the target. As the world becomes more inter-connected, it will become more difficult to influence an adversary due to the sheer numbers of information inputs relied upon to make decisions. Each source of information must either

[11] Edward Waltz, Information Warfare: Principles and Operations (Norwood: Artech House, INC, 1998), 10, 362-368.
[12] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington DC: 9 October 1998), II-3 – II-7.

be altered to support the objective of the information campaign, or isolated to create enough ambiguity to slow the decision making process. Further complications arise because the target is more sophisticated and in tune with the information environment such that gross manipulation will be suspect and likely recognized by the target.

As information-based warfare relates to information warfare, the U.S. military has been a victim of its own success. For each successive military operation during which information superiority is unchallenged, a perception emerges that information superiority will not be contested in the future. Additionally, critics claim that the concept of information warfare has been oversold, with no tangible evidence that it will achieve prominence. It has been suggested by some that the entire notion of information warfare is a transitory one.[13] In military terms, information operations have not ascended to become integral to the main effort.

The notion of information warfare has generated a great deal of study within the U.S. military establishment over the last decade. During U.S. military operations in Bosnia, Somalia, Kosovo, Afghanistan, and Iraq, significant effort was dedicated to the evolving information warfare tactics, techniques and procedures. Even with this development, the state of the art for information warfare has not significantly matured due to the following factors:

1) The U.S. military remains ostensibly a second wave force, dependent upon mass, maneuver, and industrial capabilities to overwhelm adversaries. The military is still organized, trained and equipped along service specific, platform-centric

[13] Martin C. Libicki, What Is Information Warfare? (Washington, D.C.: The Center for Advanced Concepts and Technology, National Defense University, August 1995), 18.

capabilities. Networked operations have greatly improved interoperability, but information flow continues to travel along stove-piped lines. The use of information technology has vastly improved the ability of U.S. forces to share data, but this does not constitute a mature information age capability.

2) No other information-based society has presented itself as a direct threat to U.S. power. As the Tofflers rightly infer, information age societies will field military forces that rely upon information as a key enabler.[14] Information superiority will remain uncontested until a force resourced by an information age power emerges. This is significant, as a lack of a perceived threat has lulled the U.S. military into a false sense of security. Over time information superiority will inevitably be contested.

3) From an operational planning perspective, information superiority is not well enough understood to factor into the overall campaign. Effects-based planning methods have emerged giving credence to the notion that kinetic options do not always achieve desired results, but gaining and maintaining information superiority is not typically a prime objective of the campaign. Even if a planner were to attempt to quantify the problem, there are no rules of thumb derived from real world examples or extensive war-gaming to rely upon.

Because of the above factors, information operations have not significantly altered how the U.S. military perceives it will conduct war fighting. The success of information-based operations has masked the potential benefits of using information offensively. Information operations and information warfare have not reached prominence within modern

[14] Toffler and Toffler, 73-93.

warfare. As a result, the tactics, techniques and procedures for waging information warfare remain relatively immature.

The Reliance on Information

The value of information has emerged to be pre-eminent in almost every facet of U.S. military operations. As described in Joint Vision 2020 (JV2020), information superiority is the key enabler to achieve victory.[15] Within the four war fighting concepts described by JV2020, information becomes a key variable for success, as outlined below:

1) Dominant Maneuver – Various information technologies have been employed to shape information to achieve unity of effort and an unparalleled speed of command. These advantages enable relatively small military forces freedom of maneuver to achieve positional advantage. Positioning forces relative to the enemy center of gravity is achieved through the ability of the U.S. military commander to identify critical vulnerabilities and decisive points, while avoiding mass on mass and attrition warfare courses of action. [16]

2) Precision Engagement - Information enables the commander to determine the best method to achieve a desired effect, apply the appropriate forces, and surmise the outcome of the engagement. A robust intelligence, surveillance, and reconnaissance capability enables a full range of options by developing a clear picture of enemy disposition, capabilities, limitations, and intentions. The Global Positioning System (GPS) enables reliable navigation for the commander's forces and provides

[15] Joint Chiefs of Staff, Joint Vision 2020 (Washington D.C.: Government Printing Office, June 2000), 8-9.
[16] Ibid., 20-21. Examples of information technologies include automated tactical data links, common operational picture, chat, web pages, email, computer-based office tools, and global military internets (classified and unclassified).

precision to weapons systems.[17] Dominant maneuver (enabled by information superiority) provides freedom of action to shape the battle space for engagement.

3) Focused Logistics – Transparency regarding the disposition of all supplies and the ability to control the flow of logistics is achieved via a robust data exchange network.[18] Use of networks to transport the information and web technology to allow visibility into the status of a requisition or force movement provides the commander the ability to actively manage operational logistics.

4) Full Dimension Protection - Protection from attack on critical information and systems required for operational success is described in JV2020 as a "critical need."[19] The operational level of war is the integrating level for joint operations; inter-service de-confliction to reduce fratricide is highly reliant upon information-based processes.[20]

JV2020 rightly states that information superiority is an enabler for each of the concepts described above.[21] As each of the services acquires capabilities to meet the intent of JV2020, a danger lurking is that systems and processes become *reliant upon* the information advantage. When information superiority becomes the pre-cursor to successful military operations, denial of information superiority by an enemy exposes a critical vulnerability.

Contemplating the Loss of Information Superiority

[17] GPS is a global, U.S., space-based navigation system that provides a very accurate latitude, longitude and altitude to users or systems equipped with a GPS receiver.
[18] Joint Vision 2020, 24-25.
[19] Ibid., 26-27.
[20] Joint Chiefs of Staff, An Evolving Joint Perspective: US Joint Warfare and Crisis Resolution in the 21st Century, Memorandum for the Joint Requirements Oversight Council (Washington D.C.: 28 January 2003), 3-4.
[21] Joint Vision 2020, 9.

What if information superiority were taken away? The information advantage that the U.S. military enjoys is the output of a complex, technical system of systems. If an adversary were to successfully attack this spectrum of capabilities, it could have profound impacts on the ability of U.S. forces to operate. Without information superiority, dominant maneuver becomes uncoordinated maneuver over unknown terrain, focused logistics becomes unresponsive logistics over long lines of communication, full spectrum protection degrades to local protection without indications and warning accompanied by increased fratricide, and precision engagement degrades to mass attrition scenarios with high levels of collateral damage.

How would information superiority be denied? The decentralized nature of networks presents a challenge using traditional kinetic targeting methods. Additionally, kinetic effects are often not conducive to achieving the political objectives of the operation. For example, physical destruction of a complex fiber optic network may involve targeting key nodes throughout an urban environment. This option may not be politically palatable. Even with destruction of many key nodes, the inherent nature of networks may ensure alternate routes remain intact. Attacks within the information sphere are more effective, because many nodes can be affected without having to physically destroy the equipment. This is possible due to commonality in operating systems, network addressing, and hardware that can be targeted from common links within the network.

Where is the information infrastructure vulnerable? The fundamental challenge to deny information superiority is to gain access within the right information domain. One aspect of the military information infrastructure that differs from the business world is the requirement for mobility and responsiveness. Wireless access is a driving factor in systems

design. Due to the non-persistent nature of global military operations, space-based communications, navigation, reconnaissance, and environmental satellites comprise key portions of the information domain. These systems provide global wireless access, acceptable levels of persistence, and sufficient capacity to field forces anywhere on earth with little notice.[22]

Space: Access to the Critical Vulnerability

Space provides a medium from which an adversary might attempt to exploit and subsequently deny the information advantage. The same characteristics that make space attractive for a mobile force, also provide an access point from which to attack. The radio frequency spectrum is vulnerable to unauthorized access or jamming. The level of persistence of the satellite over a target area defines windows of opportunity for the adversary to study the system and develop methodologies for attack. Finally, U.S. space-based systems provide robust capacities, but are finite in quantity. Given time to study the problem, a strategy to counter the capabilities of each space element is conceivable. The denial of the U.S. space-based capability is a lucrative and quantifiable problem for an emerging power.[23]

Denial of a significant portion of the space-based information infrastructure would result in the degradation of the shared awareness of the joint force. Loss of the unity of effort and speed of command would degrade the effectiveness of the force leading to a "leveling of the playing field" with an adversary force. Commanders may not be afforded the ability to coordinate across multiple aspects of an operation to maximize forces in time and space. The

[22] Commission to Assess United States National Security Space Management and Organization, Report of the Commission to Assess United States National Security Space Management and Organization, (Washington D.C.: 11 January 2001), 9, 12-16, 32.

smaller forces (mass) that achieved dominant maneuver and precision engagement in the past may find themselves isolated from the larger force, deep in enemy territory with contested lines of operation back to the safety of the base of operations. This scenario could be catastrophic.

A Recommended Strategy to Characterize the Problem

The line of reasoning above is meant to illustrate the vital importance of a course of action that ensures attainment of information superiority. Assumptions that oversimplify or ignore the vulnerabilities associated with information superiority are dangerous. The importance of information superiority, information operations, and information warfare has been acknowledged in joint doctrine, but the development of mature tactics, techniques and procedures to leverage these advantages and protect critical vulnerabilities remains elusive. One approach to this problem is through the use of war gaming to better understand the dynamics involved and to develop a body of knowledge about the role of information in warfare in the information age. A brief review of an historical example illustrates the point.

The U.S. Navy campaign in the Pacific in WWII was highlighted by the introduction of several maritime capabilities to include refueling at sea and aircraft carrier operations. The leadership within the navy also had developed a deep understanding of the topography and challenges of a war across a vast oceanic space. Gaining maritime superiority in the Pacific Campaign was no accident. This success can be directly related to War Plan Orange war gaming conducted by the U.S. Navy over several decades.[24]

At the conclusion of the war, Fleet Admiral Nimitz observed that the kamikaze was a complete surprise, denoting that even the most robust plans are subject to unforeseen tactics

[23] Ibid., 99-100.

by the adversary.[25] Additionally, the role of the aircraft carrier was not clearly articulated in the manner that was ultimately used during the war.[26] U.S. planners understood the importance of the evolving use of air power, even though the ways in which the force was used in battle changed over time. War-gaming proved to be a successful methodology to understand a complex campaign against a highly capable adversary.

A similar, sustained war-gaming effort is required to understand the role of information in modern warfare. Short of learning these lessons during military operations, a strategy of successive war gaming in which the opposing side is assumed to have a robust information warfare capability designed to deny U.S. information superiority is warranted. Over time, the war gaming will achieve three important objectives from a combatant commander's perspective:

1) Tactics, techniques and procedures will be developed to counter the potential of information warfare waged against U.S. information processes and to use information offensively against an information-enabled force.

2) Requirements for redundancy, authentication, and security of the information infrastructure will be refined to counter specific threats.

3) A culture of understanding warfare in the information age will be developed. This will translate to a war fighting philosophy that considers the information realm of operations equally with the other instruments of military power.

Once the U.S. military community has reached this point, the force will have fully transformed to meet the demands of the information age.

---

[24] Edward S. Miller, The U.S. Strategey to Defeat Japan 1897-1945 (Annapolis, MD: Naval Institute Press, 1991), 357-369.

Full Spectrum Red Team Concept

In order to achieve a knowledge base regarding the various aspects of the role of information in warfare, the war gaming effort requires a small cadre of subject matter experts dedicated to examining various information superiority strategies. Simulated attacks against information-based warfare capabilities are required over an extended period of time. The result will be a set of validated planning assumptions for information superiority. Additionally, tactics, techniques and procedures for offensive information warfare will be adopted for use.

This cadre, deemed the full spectrum red team, should have the charter to analyze all available methods to conduct information warfare attack. Vulnerabilities across the information sphere at the operational level of war should be examined to include: influence of the press on operational war fighting, network vulnerabilities, psychological operations, electronic warfare, operational security, and deception. These attacks should be viewed in a holistic and synergistic manner, rather than taken in isolation.

Core capabilities of the full spectrum red team should include expertise in the areas of information operations, space operations, joint operational planning and war fighting, logistics, and intelligence. Most importantly, experts with significant cultural understanding of the emerging information powers of the world must be included. The lack of cultural understanding will lead to false assumptions regarding the value a particular military force might place on the importance of information superiority. This team should be integrated into the U.S. Joint Forces Command training process[27] for Joint Task Force staffs for crisis

---

[25] Ibid., 356.
[26] Ibid., 348-350.
[27] Joint Chiefs of Staff, Unified Command Plan 2002, Memorandum for the Secretary of Defense, (Washington D.C.: 30 April 2002), 8-9.

action planning, as well as into the deliberate planning process of each of the combatant commanders.

Full spectrum red-teaming across multiple aspects of U.S. war gaming will ultimately grow the awareness and expertise of the combatant commanders and their staff officers to the point that information superiority will become a prime consideration during deliberate and crisis planning.

Conclusion: Preparing to Meet the Challenges of the Information Age

The United States has enjoyed tremendous success over the last decade integrating information-based capabilities into the force. Information superiority is central to the joint concepts envisioned for the twenty-first century U.S. fighting force. As systems are developed along the central themes of dominant maneuver, precision engagement, focused logistics, and full spectrum protection, scarce effort is currently underway to best understand the inherent vulnerabilities of information superiority.

This advantage is a fleeting one: future adversaries are likely to emulate U.S. war fighting doctrine to place information superiority as a central theme in their doctrine and develop offensive capabilities to deny information superiority to U.S. forces. Asymmetric means are likely to be used to counter the overwhelming technical and numerical advantages that the U.S. military enjoys. Information warfare provides a palatable alternative for emerging information powers to deter U.S. military intervention without having to build large standing forces. The information infrastructure relied upon to achieve information superiority by U.S. military forces today is vulnerable to attack. Space is one example of an access point that is universal to current and future military operations.

One method to maintain the information advantage is to embark upon a war-gaming strategy that methodically studies the problem using a small team of highly specialized experts. Findings from this team can be fed back into the development of new doctrine, capabilities, and policies. Most importantly, exposure to various aspects of information warfare attacks during war games will gradually transform the operational commander's understanding of the information battle space and enable operational staffs to effectively plan for the nuances of warfare in the information age.

Bibliography

Alperts, David. Information Age Transformation: Getting to a 21st Century Military. Washington D.C.: Government Printing Office, June 2002.

Alberts, David S. and Richard E. Hayes. Power to the Edge: Command and Control in the Information Age. Washington D.C.: Government Printing Office, June 2003.

Berkowitz, Bruce. The New Face of War: How War Will Be Fought in the 21st Century. New York: The Free Press, Simon & Shuster, 2003.

Brennen, Rick and R. Evan Ellis. Information Warfare in Mulitlateral Peace Operations: A Case Study of Somalia, Washington D.C.: Science Applications International Corporation, 18 April 1996

Commission to Assess United States National Security Space Management and Organization. Report of the Commission to Assess United States National Security Space Management and Organization. Washington D.C.: 11 January 2001

Gerard, Phillip. Secret Soldiers: The story of WWII's secret army of deception. New York: Dutton, 2002.

Jones, Andy, Gerald L. Kovacich, and Perry G. Luzwick. Global Information Warfare. Boca Raton, FL: Auerbach Publications, 2002.

Libicki, Martin C. Defending Cyberspace and other Metaphors. Washington, D.C.: The Center for Advanced Concepts and Technology, National Defense University, February 1997.

_____. Illuminating Tomorrow's War. Washington, D.C.: McNair Paper, no. 61. Institute for National Strategic Studies, National Defense University, October 1999.

_____. What is Information Warfare?. Washington, D.C.: The Center for Advanced Concepts and Technology, National Defense University, August 1995.

McClanahan, Jack R. Jr. America's Information War on Terrorism: Winning Hearts and Minds in the Muslim World. Carlisle, PA: US Army War College, 27 Mar 2002.

Miller, Edward S. The U.S. Strategey to Defeat Japan 1897-1945. Annapolis, MD: Naval Institute Press, 1991.

Potter, E.B. Nimitz: A Biography. Annapolis, MD: Naval Institute Press, 1976.

Rattray, Gregory J. Strategic Warfare in Cyberspace. Boston: Massachusetts Institute of Technology, 2001.

Toffler, Alvin. The Third Wave. New York: William Morrow and Company, 1980.

Toffler, Alvin and Heidi Toffler. War and Anti-War: Making Sense of Today's Global Chaos. New York: Warner Books, 1993.

U.S. Joint Chiefs of Staff. Department of Defense Dictionary of Military and Associated Terms. Joint Pub 1-02. Washington, D.C.: Government Printing Office, 12 April 2001 (as amended through 5 June 2003).

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub 3-0. Washington D.C.: Government Printing Office, 10 September 2001.

_____. Doctrine for Information Operations. Joint Pub 3-13. Washington D.C.: Government Printing Office, 9 October 1998.

_____. An Evolving Joint Perspective: US Joint Warfare and Crisis Resolution in the 21st Century. Memorandum for the Joint Requirements Oversight Council. Washington D.C.: Government Printing Office, 28 January 2003.

_____. Joint Vision 2020. Washington D.C.: Government Printing Office, June 2000.

_____. Unified Command Plan 2002. Memorandum for the Secretary of Defense. Washington D.C.: 30 April 2002.

Walz, Edward. Information Warfare Principles and Operations. Norwood: Artech House, 1998.